UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

DAVID BISHOP, on behalf of himself and all others similarly situated, Plaintiff, v. MAXIMUS FEDERAL SERVICES, INC., Defendant.	Case No. 1:23-cv-1019 **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff David Bishop, individually and on behalf of all similarly situated persons, alleges the following against MAXIMUS Federal Services, Inc. ("Maximus" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents, as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Maximus for its failure to properly secure and safeguard Plaintiff's and other similarly situated patients' sensitive information, including full names; dates of birth, addresses, contact information, driver's license numbers, and Social Security numbers, ("personally identifiable information" or "PII") and medical and health insurance information, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

2. Defendant assists health agencies in administering and delivering services, including to Medicare patients. Defendant provides medical evaluations, review of eligibility

appeals, enrollment assistance, data analysis, and IT and consulting services.[1] Regarding Medicare specifically, Defendant reviews "more than 600,000 appeals claims a year for Medicare" patients who experienced health insurance denials.[2]

3. Upon information and belief, former and current Medicare patients are required to entrust Defendant with sensitive, non-public Private Information, without which Defendant could not perform its regular business activities, in order to obtain medical services from Medicare. Defendant retains this information for at least many years and even after the patient-physician relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or about May 30, 2023, Defendant "detected unusual activity in its MOVEit application."[3] In response, Defendant "began to investigate" into the scope and nature of the Data Breach.[4] As a result of its investigation, which is ongoing, Defendant concluded that Plaintiff's and Class Members' Private Information was compromised in the Data Breach.[5]

6. According to Defendant's untitled letter sent to Plaintiff and Class Members (the "Notice Letter"), the compromised Private Information included individuals' names; dates of birth; addresses; contact information; driver's license numbers; Social Security numbers; Medicare beneficiary identifiers or health insurance claim numbers; healthcare providers and prescription

[1] https://maximus.com/our-company (last accessed July 31, 2023).
[2] https://maximus.com/cms (last accessed July 31, 2023).
[3] The "Notice Letter". A sample copy is available at https://www.cms.gov/newsroom/press-releases/cms-responding-data-breach-contractor (last accessed July 31, 2023).
[4] *Id.*
[5] *Id.*

information, health insurance claims and policy/subscriber information, health benefits and enrolment information, and medical histories/notes, including medical records/account numbers, conditions, diagnoses, dates of service, images, treatment, and other sensitive information.

7. Defendant failed to adequately protect Plaintiff's and Class Members Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect patients' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

9. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by its IT vendors to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal

use. As a result, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

10. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) Plaintiff experiencing misuse of his PII in the form of an identity thief using his PII to apply for an Allstate auto insurance policy in or about July 2023; (ii) Plaintiff's CreditKarma account being accessed by an identity thief in or about July 2023; (iii) an increase in unauthorized credit inquiries on Plaintiff's credit report; (iv) invasion of privacy; (v) lost or diminished value of Private Information; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

11. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

II. PARTIES

12. Plaintiff David Bishop, is, and at all times mentioned herein was, an individual citizen of Brick, New Jersey.

13. Defendant MAXIMUS Federal Services, Inc. is a Virginia corporation with its principal place of business located at 1600 Tysons Boulevard McLean, VA 22102

III. JURISDICTION AND VENUE

14. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the state of Virginia and have different citizenship from Maximus, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A)

15. This Court has jurisdiction over Maximus because Maximus operates in this District.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Maximus has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

Defendant's Business

17. Defendant assists health agencies in administering and delivering services, including to Medicare patients. Defendant provides medical evaluations, review of eligibility appeals, enrollment assistance, data analysis, and IT and consulting services.[6] Regarding Medicare specifically, Defendant reviews "more than 600,000 appeals claims a year for Medicare" patients who experienced "health insurance denials."[7] Defendant is the largest provider of government-

[6] https://maximus.com/our-company (last accessed July 31, 2023).
[7] https://maximus.com/cms (last accessed July 31, 2023).

sponsored benefit appeals programs in the United States

18. Defendant currently employs approximately 39,000 individuals and generates more than four billion dollars in annual revenue.[8]

19. Plaintiff and Class Members are current and former Medicare patients, who were required to provide their Private Information, directly or indirectly, to Defendant.

20. As a condition of receiving products and/or services, Maximus requires that Medicare patients, including Plaintiff and Class Members, entrust it with highly sensitive personal information.

21. The information held by Defendant in its computer systems or shared with its vendors at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

22. Upon information and belief, Defendant made promises and representations to its Medicare patients, including Plaintiff and Class Members, that the Private Information collected from them as a condition of obtaining products and/or services at Medicare would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

23. Indeed, Defendant's Privacy Statement provides that: “Maximus uses various technological and procedural security measures in order to protect the personal information we collect through the Site from loss, misuse, alteration or destruction. We have documented Information Security & Privacy policies to address data protection. We regularly provide information security and privacy awareness training to our employees."[9]

[8] https://maximus.com/our-company (last accessed July 31, 2023).
[9] https://maximus.com/privacy-statement (last visited July 31, 2023).

24. Plaintiff and Class Members provided their Private Information to Defendant, directly or indirectly, with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

25. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

26. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors' and affiliates' data security practices and systems. Defendant has a legal duty to keep patient's Private Information safe and confidential.

27. Defendant had obligations created by FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

28. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private

Information from disclosure.

The Data Breach

30. On or about July 28, 2023, Defendant began sending Plaintiff and other Data Breach victims an untitled (the "Notice Letter"), informing them that:

What Happened?

On May 30, 2023, Maximus detected unusual activity in its MOVEit application. Maximus began to investigate and stopped all use of the MOVEit application early on May 31, 2023. Later that same day, the third-party application provider, Progress Software Corporation, announced that a vulnerability in its MOVEit software had allowed an unauthorized party to gain access to files across many organizations in both the government and private sectors.

Maximus notified CMS of the incident on June 2, 2023. To date, the ongoing investigation indicates that on approximately May 27 through 31, 2023, the unauthorized party obtained copies of files that were saved in the Maximus MOVEit application, but that no CMS system has been compromised. After notifying CMS, Maximus then began to analyze the files to determine which data had been affected. As part of that analysis, it was determined that those files contained some of your personal information.

What Information Was Involved?

We have determined that your personal and Medicare information was involved in this incident. This information may have included the following:

- Name
- Social Security Number or Individual Taxpayer Identification Number
- Date of Birth
- Mailing Address
- Telephone Number, Fax Number, & Email Address
- Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
- Driver's License Number and State Identification Number
- Medical History/Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.)
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information
- Health Benefits & Enrollment Information.[10]

[10] Notice Letter.

31. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed. Moreover, Defendant failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share sensitive Private Information.

32. The attacker accessed and acquired files Defendant shared with a third party containing unencrypted Private Information of Plaintiff and Class Members, including their Social Security numbers, PHI, and other sensitive information. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

33. Plaintiff further believes his Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

34. Defendant could have prevented this Data Breach by, among other things, properly encrypting Private Information being shared with its vendors or otherwise ensuring that such Private Information was protected while in transit or accessible.

35. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

36. The unencrypted Private Information of Class Members will end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed Private Information for targeted marketing without the

approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

Defendant Acquires, Collects, And Stores Medicare Patients' Private Information

37. As a condition to obtain products and/or services from Medicare, Plaintiff and Class Members were required to give their sensitive and confidential Private Information, directly or indirectly, to Defendant.

38. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to perform its services.

39. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

40. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

41. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members or by exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

42. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

43. Indeed, Defendant's Privacy Statement provides that: "Maximus uses various technological and procedural security measures in order to protect the personal information we collect through the Site from loss, misuse, alteration or destruction. We have documented Information Security & Privacy policies to address data protection. We regularly provide information security and privacy awareness training to our employees."[11]

44. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk Because Medicare Contractors In Possession Of Private Information Are Particularly Suspectable To Cyber Attacks

45. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting Medicare contractors and health care services providers that collect and store Private Information, like Defendant, preceding the date of the breach.

46. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

47. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[12]

48. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive

[11] https://maximus.com/privacy-statement (last visited July 31, 2023).
[12] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[13]

49. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[14]

50. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[15] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[16] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[17]

51. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients,

---

[13] *Id*.

[14] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Oct. 17, 2022).

[15] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

[16] *Id*.

[17] *Id*.

September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals

52. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[18]

53. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in 2019 alone.[19]

54. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

55. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

56. At all relevant times, Defendant knew, or reasonably should have known, of the

[18] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware (last visited Sep. 13, 2022).

[19] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited on March 10, 2022).

importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

57. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially hundreds of thousands of individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

58. Additionally, as companies became more dependent on computer systems to run their business,[20] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[21]

59. In the Notice Letter, Defendant offers to provide 24 months of credit monitoring and identity theft insurance services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members' Private Information. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

60. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and

[20]https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[21] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

Class Members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

61. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

62. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

63. As a Medicare contractor in possession of current and former Medicare patients' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

F. ***Value Of Personally Identifiable Information***

64. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[22] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

[22] 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number."[23]

65. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[24]

66. For example, PII can be sold at a price ranging from $40 to $200.[25] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[26]

67. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[27]

68. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[28]

69. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file),

---

[23] *Id.*
[24] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).
[25] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).
[26] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).
[27] *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, *available at:* https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658 (last visited July 31, 2023).
[28] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited on Feb. 21, 2023).

> doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

70. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[29] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[30]

71. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[31]

72. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

73. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names, PHI, and Social Security numbers.

74. This data demands a much higher price on the black market. Martin Walter, senior

---

[29] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited on Feb. 21, 2023).
[30] *Id.*
[31] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited on Feb. 21, 2023).

director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[32]

75. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[33]

Maximus Failed to Comply with FTC Guidelines

76. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for patients' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

77. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The

---

[32] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 17, 2022).

[33] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

guidelines note that businesses should protect the personal patient information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

78. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

80. These FTC enforcement actions include actions against healthcare companies, like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (Henry Ford) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

81. As evidenced by the Data Breach, Maximus failed to properly implement basic

data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Maximus's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

82. Maximus was at all times fully aware of its obligation to protect the Private Information of the Medicare patients in its network yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Maximus Failed to Comply with HIPAA Guidelines

83. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

84. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[34] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

85. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

86. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health

[34] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

information that is kept or transferred in electronic form.

87. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

88. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

89. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

90. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

91. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

92. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[35]

93. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

94. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

95. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to

[35] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[36] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[37]

Maximus Failed to Comply with Industry Standards

96. As noted above, experts studying cybersecurity routinely identify medical services administrators as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

97. Some industry best practices that should be implemented by medical services administrators dealing with sensitive Private Information, like Maximus, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

98. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in

[36] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[37] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

reasonable cybersecurity readiness.

99. Defendant failed to comply with these accepted standards in the medical services industry, thereby permitting the Data Breach to occur.

Maximus Breached its Duty to Safeguard Medicare Patients' Private Information

100. In addition to its obligations under federal and state laws, Maximus owed a duty to Plaintiff and Class Members to exercise reasonable care in sharing, obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Maximus owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

101. Maximus breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Maximus's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

e. Failing to sufficiently train its employees and vendors regarding the proper

handling of its patients Private Information;

f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

g. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and

h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

102. Maximus negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

103. Had Maximus remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

Common Injuries & Damages

104. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; I invasion of

privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

The Data Breach Increases Victims' Risk Of Identity Theft

105. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

106. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

107. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

108. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

109. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social

engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

110. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[38]

111. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

112. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still

[38] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

113. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiff and the other Class Members.

114. Thus, even if certain information (such as financial account information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

115. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

116. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

117. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant's Notice Letter instructs,[39] "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

118. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result

[39] Notice Letter.

of the Data Breach, such as researching and verifying the legitimacy of the Data Breach, changing passwords and resecuring their own computer networks, obtaining new health insurance cards, placing security measures on their accounts, and contacting numerous health care providers to correct insurance issues and ensure they do not experience medical and/or other fraud.

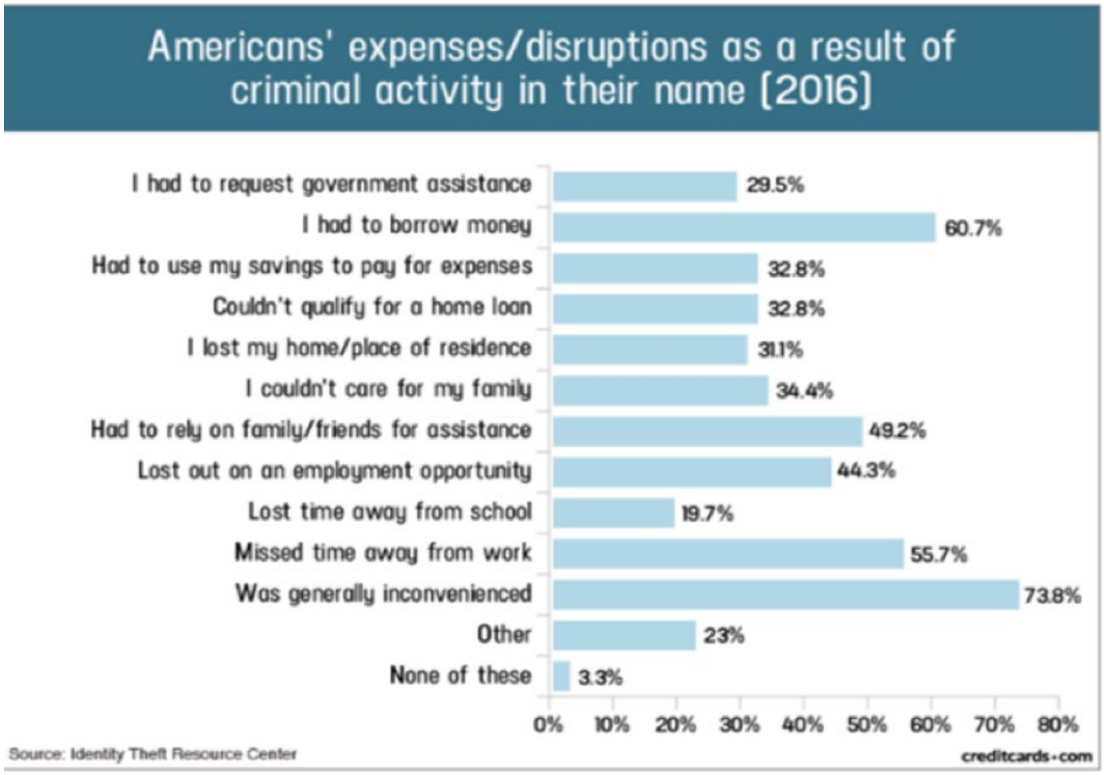
119. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[40]

120. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[41]

121. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[42]

---

[40] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[41] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[42] Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Sep 13, 2022).



122. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[43]

Diminution Value Of Private Information

123. PII and PHI are valuable property rights.[44] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy

[43] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").
[44] *See, e.g.,* Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

124. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[45]

125. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[46,47]

126. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[48]

127. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[49]

128. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

129. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[50]

---

[45] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[46] https://datacoup.com/
[47] https://digi.me/what-is-digime/
[48] Nielsen Computer & Mobile Panel, *Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html
[49] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).
[50] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)

130. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

131. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., names, PHI, and Social Security numbers.

132. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

133. The fraudulent activity resulting from the Data Breach may not come to light for years.

134. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

135. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to hundreds of thousands of individuals' detailed personal information, upon information and belief, and thus, the significant

number of individuals who would be harmed by the exposure of the unencrypted data.

136. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

137. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

138. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or his Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

139. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

140. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for

Defendant's failure to safeguard their Private Information.

Plaintiff Bishop's Experience

141. Plaintiff David Bishop is a current Medicare patient and has been more than a decade.

142. In order to obtain medical services through Medicare, he was required to provide his Private Information to Defendant, directly or indirectly, including his name, Social Security number, date of birth, contact information, health insurance information, and other sensitive information.

143. At the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Defendant retained Plaintiff's Private Information in its system and shared it with its IT vendors.

144. Plaintiff Bishop is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

145. Plaintiff David Bishop received the Notice Letter, by U.S. mail, directly from Defendant, dated July 28, 2023. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his name; Social Security number or individual taxpayer identification number; date of birth; mailing address; telephone number, fax number, & email address; Medicare beneficiary identifier (MBI) or health insurance claim number (HICN); driver's license number and state identification number; medical history/notes (including medical record/account numbers, conditions, diagnoses, dates of service,

images, treatments, etc.); healthcare provider and prescription information; health insurance claims and policy/subscriber information; and health benefits & enrollment information.

146. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, changing passwords and resecuring their own computer networks, obtaining new health insurance cards, placing security measures on their accounts, and contacting numerous health care providers to correct insurance issues and ensure they do not experience medical and/or other fraud. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

147. As a result of the Data Breach, Plaintiff has experienced the attempted misuse of his Private Information. Following the Data Breach, Plaintiff has been notified of an attempt to access his CreditKarma account and has noticed suspicious inquiries on his credit report regarding activity he did not authorize.

148. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) experiencing misuse of his PII in the form of an identity thief using his PII to apply for an Allstate auto insurance policy in or about July 2023; (ii) his CreditKarma account being accessed by an identity thief in or about July 2023; (iii) an increase in unauthorized credit inquiries on his credit report; (iv) invasion of privacy; (v) lost or diminished value of Private Information; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; and (viii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b)

remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

149. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

150. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

151. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

152. Plaintiff David Bishop has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ACTION ALLEGATIONS

153. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

154. Specifically, Plaintiff proposes the following Nationwide Class, subject to amendment as appropriate:

Nationwide Class

All individuals in the United States whose Private Information was impacted as a result of the Data Breach (the "Class").

155. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom

this case is assigned as well as their judicial staff and immediate family members.

156. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class, as well as add subclasses, before the Court determines whether certification is appropriate.

157. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

158. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Although the precise number of Class Members is unknown to Plaintiff, according to the Center for Medicare and Medicaid Services, approximately 612,0000 persons were impacted in the Data Breach, satisfying numerosity.[51]

159. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Maximus engaged in the conduct alleged herein;

b. Whether Maximus's conduct violated the FTCA and/or HIPAA;

c. When Maximus learned of the Data Breach;

d. Whether Maximus's response to the Data Breach was adequate;

e. Whether Maximus unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Maximus failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private

[51] https://www.cms.gov/newsroom/press-releases/cms-responding-data-breach-contractor (last accessed July 31, 2023).

Information compromised in the Data Breach;

g. Whether Maximus's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Maximus's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Maximus owed a duty to Class Members to safeguard their Private Information;

j. Whether Maximus breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Maximus had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Maximus breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Maximus knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Maximus's misconduct;

p. Whether Maximus's conduct was negligent;

q. Whether Maximus was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

160. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of Maximus. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

161. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

162. Predominance. Maximus has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Maximus's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

163. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered

in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Maximus. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

164. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Maximus has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

165. Finally, all members of the proposed Class are readily ascertainable. Maximus has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Maximus.

VI. CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf Of Plaintiff And The Class)

166. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

167. Defendant requires the Medicare patients in its network, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing its

services.

168. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business of soliciting its services to Medicare patients, which solicitations and services affect commerce.

169. Plaintiff and Class Members entrusted Defendant with their Private Information, directly or indirectly, with the understanding that Defendant would safeguard their information.

170. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

171. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

172. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

173. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to

protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

174. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

175. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and the Medicare patients in its network. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of receiving Medicare services.

176. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

177. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

178. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information it was no longer required to retain pursuant to regulations.

179. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

180. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been

compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

181. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to adequately monitor the security of their IT vendors' and affiliates' networks and systems to ensure they enacted reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

182. Defendant violated Section 5 of the FTC Act and HPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

183. Plaintiff and the Class are within the class of persons that the FTC Act and HIPAA intended to protect.

184. The harm that occurred as a result of the Data Breach is the type of harm that the FTC Act and HIPAA intended to guard against.

185. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

186. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

187. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

188. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the health insurance industry.

189. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were

wrongfully disclosed.

190. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

191. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

192. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

193. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

194. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

195. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

196. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

197. There is a close causal connection between Defendant's failure to implement

security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

198. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) Plaintiff experiencing misuse of his PII in the form of an identity thief using his PII to apply for an Allstate auto insurance policy in or about July 2023; (ii) Plaintiff's CreditKarma account being accessed by an identity thief in or about July 2023; (iii) an increase in unauthorized credit inquiries on Plaintiff's credit report; (iv) invasion of privacy; (v) lost or diminished value of Private Information; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

199. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

200. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private

Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

201. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

202. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

203. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf Of Plaintiff And The Class)

204. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

205. Plaintiff alleges this negligence *per se* theory as alternative to his other negligence claim.

206. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

207. Defendant's duty to use reasonable security measures also arose under the HIPAA, under which they were required to protect the security, confidentiality, and integrity of patient

information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

208. Defendant owed a duty of care in protecting Plaintiff's and Class Members' Private Information, pursuant to Section 5 of the FTC Act, HIPAA, and an independent duty of care.

209. Defendant further owed a duty, pursuant to the Virginia Data Breach Notification Law, to disclose without unreasonable delay any breach of its security systems upon discovery or notification of breach. Virginia Code § 18.2-186.6(B). Notice must go to the Office of the Attorney General and any affected Virginia Resident.

210. Defendant violated Section 5 of the FTC Act, HIPAA, Virginia Data Breach Notification Law, and similar state statutes by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

211. In its Privacy Statement, FMB promises Medicare patients that it will not disclose patients' Private Information, outside of the excepted circumstances set forth therein—none of which apply here. However, Plaintiff's and Class Members' Private Information has been disclosed without their written authorization as a result of the Data Breach.

212. Through its Privacy Statement, and in light of the highly sensitive and personal nature of the information FMB acquires and stores with respect to the Medicare patients in its network, FMB promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; and regularly provide information

security and privacy awareness training to its employees.

213. As evidenced by the occurrence of the Data Breach, Defendant negligently misrepresented its data security measures and Privacy Statement to Plaintiff and Class Members.

214. Defendant violated Section 5 of the FTC Act and HIPAA by negligently misrepresenting its data security practices to Plaintiff and Class Members.

215. Defendant violated Section 5 of the FTC Act, HIPAA, and the Virginia Data Breach Notification Law by breaching its duties of care to Plaintiff and Class Members, as provided in its Privacy Statement.

216. Defendant further violated Section 5 of the FTC Act and HIPAA by failing to ensure that its vendors use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and shared and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

217. Defendant's violation of Section 5 of the FTC Act, HIPAA, the Virginia Data Breach Notification Law, and other duties (listed above) constitutes negligence *per se.*

218. Class members are patients within the class of persons that Section 5 of the FTC Act, HIPAA, Virginia Data Breach Notification Law, and similar state statutes intended to protect.

219. Moreover, the harm that has occurred is the type of harm that the FTC Act, HIPAA, Virginia Data Breach Notification Law, and similar state statutes were intended to guard against. Indeed, the FTC has pursued over numerous enforcement actions against health insurance administrators which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class

Members.

220. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

221. There is a close causal connection between Defendant's failure to implement or ensure security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

222. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) Plaintiff experiencing misuse of his PII in the form of an identity thief using his PII to apply for an Allstate auto insurance policy in or about July 2023; (ii) Plaintiff's CreditKarma account being accessed by an identity thief in or about July 2023; (iii) an increase in unauthorized credit inquiries on Plaintiff's credit report; (iv) invasion of privacy; (v) lost or diminished value of Private Information; (vi) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) loss of benefit of the bargain; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

223. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including,

but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

224. As a direct and proximate result of Defendant's negligence *per se*, the products and/or services that Defendant provided to Plaintiff and Class Members damaged other property, including the value of their Private Information.

225. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

226. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

227. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

228. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT III
Breach of Third-Party Beneficiary Contract
(On Behalf Of Plaintiff And The Class)

229. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

230. Defendant entered into written contracts, including HIPAA Business Associate

Agreements, with Medicare to provide management and administrative services.

231. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

232. These contracts were made expressly for the benefit of Plaintiffs and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and Medicare. Defendant knew that, if it were to breach these contracts with Medicare, the Medicare patients—Plaintiffs and Class Members—would be harmed.

233. Defendant breached the contracts it entered into with Medicare by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiff and Class Members of the Data Breach.

234. Plaintiff and the Class were harmed by Defendant's breach of its contracts with Medicare, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

235. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT IV
Unjust Enrichment
(On Behalf Of Plaintiff And The Class)

236. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

237. This Count is brought in the alternative to the breach of third party beneficiary contract count above.

238. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

239. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form their Private Information as well as payments made on their behalf as a necessary part of their receiving healthcare services through Medicare. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

240. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

241. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

242. Defendant, however, failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

243. Defendant would not be able to carry out an essential function of its regular

business without the Private Information of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

244. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

245. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

246. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

247. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

248. Plaintiff and Class Members have no adequate remedy at law.

249. As a direct and proximate result of Defendant's conduct, Plaintiff and Class

Members have suffered and will continue to suffer other forms of injury and/or harm.

250. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: August 31, 2023 Respectfully submitted,

By:/s/ *Lee A. Floyd*
Lee A. Floyd (VSB #88459)
Sarah G. Sauble (VSB #94757)
BREIT BINIAZAN, PC
2100 E. Cary Street, Suite 310
Richmond, Virginia 23223
(804) 351-9040
(757) 670-3939
Lee@bbtrial.com
Sarah@bbtrial.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Counsel for Plaintiff and the Proposed Class

**Pro Hac Vice* application forthcoming

CERTIFICATE OF SERVICE

I hereby certify that on August 31, 2023, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ Lee A. Floyd
Lee A. Floyd (VSB #88459)
BREIT BINIAZAN, PC